IN THE CLAIMS

The listing of claims will replace all prior versions, and listing, of claims in the application:

Claim 1 (currently amended) A method of providing a digital file from a source system to ~~an~~ certain embedded systems in a secure manner, the digital file including instructions for configuring and operating the embedded systems, comprising the steps of:

combining the digital file with a header ~~information~~ including ~~a target identifier corresponding to the~~ target state information specifying a certain embedded system;

providing the combined digital file with the header ~~information~~ to the embedded system; ~~and~~

verifying the ~~target identifier~~ target state information upon receipt of the digital file at the embedded system;

~~before the embedded system is enabled to install said digital file on the embedded system~~ installing the digital file on the embedded system only if the target state information in the header corresponds to target state information of the embedded system; and

operating the embedded system using the digital file until a further updated version of the digital file is installed on the embedded system.

Claim 2 (currently amended) The method as defined in claim 1 wherein the ~~target identifier~~ target state information is a text name corresponding to an end user of an Internet based service.

Claim 3 (currently amended) The method as defined in claim 1 wherein said ~~target identifier~~ target state information includes a revision level respecting said digital file.

Claim 4 (previously amended) A method of providing a digital file from a source system to ~~an~~ certain embedded systems in a secure manner, the digital file including instructions for configuring and operating the embedded systems, comprising the steps of:

combining the digital file with a header ~~information~~ including ~~a target identifier corresponding to the~~ target state information specifying a certain embedded system;

signing the combined digital file with the header ~~information~~ with a digital signature corresponding to the source system, the digital signature being added to the header ~~information~~;

providing the combined digital file with header ~~information~~ to the embedded system; ~~and~~

verifying the digital signature and the target ~~identifier~~ state information upon receipt of the digital file at the embedded system;

installing the digital file on the embedded system only if the target state information in the header corresponds to target state information of the embedded system and if the digital signature is verified; and ~~before the embedded system is enabled to install the digital file on the embedded system~~

operating the embedded system using the digital file until a further updated version of the digital file is installed on the embedded system.

Claim 5 (currently amended) The method as defined in claim 4, wherein the step of signing the combined digital file with a header ~~information~~ uses a private cryptographic key associated with the source system to generate the digital signature.

Claim 6 (original) The method as defined in claim 5 wherein the step of verifying the digital signature uses a public key corresponding to the private cryptographic key.

Claim 7 (currently amended) An embedded system that uses ~~a target state header~~ target state information to validate uploaded files, the system comprising:

means to combine the files to be uploaded with the target state information specifying the embedded system ~~header~~;

means to provide the files with the target state information ~~header~~ to the embedded system; ~~and~~

verifying means to verify the target state information; and ~~header~~

means to install the digital file on the embedded system only if the target state information which has been combined with the files corresponds to target state information of the embedded system ~~before the files are installed on the embedded system~~.

Claim 8 (previously amended) The embedded system as defined in claim 7 having means to provide a digital signature for use in verifying the files before installing the files on the embedded system.

Claim 9 (original) The embedded system as defined in claim 8 having public keying infrastructure for distributing public keying information to said embedded system.

Claim 10 (original) The embedded system as defined in claim 9 having software for performing signature generation and verification.

Claim 11 (original) The embedded system as defined in claim 7 for use in conducting transactions on the Internet.

Claim 12 (original) The embedded system as defined in claim 11 wherein said transactions include the purchase and download of software.

Claim 13 (original) The embedded system as defined in claim 11 wherein said transactions include online banking.

Claim 14 (original) The embedded system as defined in claim 11 wherein said transactions include the installation of software revisions in network nodes.

Claim 15 (previously amended) The embedded system as defined in claim 14 wherein said network nodes include wireless telephones.